sub a2

WHAT IS CLAIMED IS:

1. A cryptographic communication terminal comprising:

a cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication, and outputting a designated cryptographic algorithm;

a key information storage section for storing a key used for cryptographic communication corresponding to the cryptographic algorithm, and outputting a designated key;

control means for designating, with respect to said cryptographic algorithm storage section and said key information storage section, which cryptographic algorithm and key are to be used in the cryptographic communication; and

encryption/decryption means for decrypting received encryption information by using the cryptographic algorithm designated with respect to said cryptographic algorithm storage section and the key designated with respect to said key information storage section, and encrypting information to be transmitted.

2. A terminal according to claim 1, wherein said cryptographic algorithm storage section stores an encrypted cryptographic algorithm, and

said terminal further comprises cryptographic algorithm decryption means for decrypting the encrypted

cryptographic algorithm.

3. A terminal according to claim 2, wherein said key information storage section stores a key for an encrypted algorithm used to decrypt an encrypted cryptographic algorithm as well as the key for cryptographic communication.

4. A terminal according to claim 3, wherein the key for the encrypted algorithm is a key for secret key cryptography.

5. A terminal according to claim 3, wherein the key for the encrypted algorithm is a key for public key cryptography.

6. A terminal according to claim 1, wherein said key information storage section stores an encrypted key, and

said terminal further comprises key information decryption means for decrypting the encrypted key.

7. A terminal according to claim 1, wherein said control means instructs said cryptographic algorithm storage section to output a requested cryptographic algorithm upon receiving a transmission request for any one of the cryptographic algorithms stored in said cryptographic algorithm storage section, and

said encryption/decryption means encrypts the requested cryptographic algorithm as the information to be transmitted.

8. A terminal according to claim 1, wherein when

a partner with which said terminal communicates is an apparatus including said cryptographic communication terminal, said terminal requests the partner for a new cryptographic algorithm and/or a key for a corresponding encrypted algorithm, decrypts a corresponding response by using said encryption/decryption means,

stores the requested cryptographic algorithm in said cryptographic algorithm storage section upon receiving the cryptographic algorithm, and stores the requested key for the encrypt algorithm in said key information storage section upon receiving the key.

9. A cryptographic communication center apparatus comprising said cryptographic communication terminal defined in claim 3, wherein when the algorithm decryption key is requested from the partner, said apparatus inputs the corresponding algorithm decryption key as the information to be transmitted to the partner to said encryption/decryption means.

10. An apparatus according to claim 9, wherein said apparatus comprises said cryptographic communication terminal defined in claim 3, and an update cryptographic algorithm storage section for storing a plurality of types of cryptographic algorithms decrypted by using a key for the encrypted algorithm, and

said control means, when a cryptographic algorithm is requested from said cryptographic communication

terminal, instructs said update cryptographic algorithm storage section, in place of said cryptographic algorithm storage section, to output the requested cryptographic algorithm as the information to be transmitted.

11. An apparatus according to claim 9, further comprising key encrypt means for, when the key for the encrypted algorithm is requested from said cryptographic communication terminal, encrypting the key for the encrypted algorithm to be transmitted, and inputting the encrypted key for the encrypted algorithm, as the information to be transmitted, to said encryption/decryption means.

12. An apparatus according to claim 11, wherein said key encryption means encrypts the key for the encrypted algorithm by using a key unique to a cryptographic communication terminal of the partner.

13. A cryptographic communication system comprising not less than two cryptographic communication terminals each defined in claim 1.

14. A cryptographic communication center apparatus comprising not less than one cryptographic communication terminal defined in claim 1 and not less than one cryptographic communication center apparatus defined in claim 7.

15. A computer readable medium storing a program for implementing:

a cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication, and outputting a designated cryptographic algorithm;

a key information storage section for storing a key used for cryptographic communication corresponding to the cryptographic algorithm, and outputting a designated key;

control means for designating, with respect to said cryptographic algorithm storage section and said key information storage section, which cryptographic algorithm and key are to be used in the cryptographic communication; and

encryption/decryption means for decrypting received encryption information by using the cryptographic algorithm designated with respect to said cryptographic algorithm storage section and the key designated with respect to said key information storage section, and encrypting information to be transmitted.

16. A storage according to claim 15, wherein said cryptographic algorithm storage means further comprises a program for storing an encrypted cryptographic algorithm, and

implementing cryptographic algorithm decryption means for decrypting the encrypted algorithm by using a key for the encrypted algorithm.

17. A storage according to claim 15, wherein said

control means further comprises a program for, when a transmission request for any of the cryptographic algorithms stored in said cryptographic algorithm storage means is received, instructing said cryptographic algorithm storage means to output the requested cryptographic algorithm, and

said encryption/decryption means further comprises a program for encrypting the requested cryptographic algorithm as the information to be transmitted.

18. A storage according to claim 16, further comprising a program for, when a key for the encrypted algorithm is requested from the partner, inputting the corresponding key for the encrypted algorithm, as the information to be transmitted to the partner, to said encryption/decryption means.

19. A cryptographic communication center apparatus having said storage medium defined in claim 16, comprising:

update cryptographic algorithm storage means for storing a plurality of types of cryptographic algorithms encrypted by the key for the encrypted algorithm; and

means for, when the cryptographic algorithm decryption key is requested from the partner, inputting a corresponding key for the encrypted algorithm, as information to be transmitted to the partner, to said encryption/decryption means,

wherein said control means stores a program for, when a cryptographic algorithm is requested from said cryptographic communication terminal, instructing said update cryptographic algorithm storage means to output the requested cryptographic algorithm as the information to be transmitted.

20. A system according to claim 13, wherein said cryptographic communication terminal acquires the cryptographic algorithm and a decryption key therefor from said cryptographic communication center apparatus.

21. A system according to claim 11, wherein said cryptographic communication terminal acquires a cryptographic algorithm from another cryptographic communication terminal and acquires a corresponding decryption key from said cryptographic communication center apparatus.